

Below are several recent e-news items that may be of interest.

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Many thanks to all who contributed to this information!!!
Have a great day!!!
Ken

Items included below are:

- ISSA Conference change
- [hipaalive] Requirements for e-processing
- [hipaalive] Clearinghouse Document
- [hipaalive] IDENTIFIERS: Provider ID
- [hipaalive] PHI Disclosure
- [hipaalive] PRIVACY: Emailing of Patient Information
- HIPAAALERT - I i t e Sept 25, 2001

***** ISSA Conference change

The Sacramento Valley chapter of the
Information Systems Security Association (ISSA)
Invites you to register for -

The 12th Annual Northern California
Information Security Conference

"InfoSeCon 2001" Wednesday October 3, 2001

Please see the attachment for agenda and registration information.

***** Requirements for e-processing

*** This is HIPAAlive! From Phoenix Health Systems ***

Providers that conduct electronically any transaction for which HIPAA has established a standard, will have to use HIPAA standards for those electronic transactions. They may modify their own systems, or use a clearinghouse, to do this. However, unlike health plans, they aren't required to perform the transactions electronically. Health plans don't have the option of being "paper only" shops. Providers do, at least under HIPAA. Whether that makes good business sense is another matter.

As a PBM, you may not be a covered entity, if you are not an insurance

issuer or HMO. However, you are certainly acting as a BA to covered health plans (insurance companies, HMOs and group health plans), all of which will be required to conduct their electronic transactions in HIPAA standard form. Their contract with you, as the BA through whom they are meeting this requirement for prescription claims, will have to impose that same requirement on you. See section 162.923(c).

So the health plans which whom you do business will be prohibited by HIPAA from continuing to contract with you unless you agree, contractually, to conduct HIPAA standard transactions on their behalf.

If a provider insists on conducting a HIPAA transaction in non-standard format, they must do so through a clearinghouse. Since this is at their option and not yours (or the health plan for whom you are providing services), you are not required to bear the clearinghouse fees. BTW, the rules say that the health plan, not the health plan's BA, is responsible for clearinghouse fees when the health plan (or the BA on behalf of the health plan) requires providers to use a clearinghouse to conduct standard transactions with it.

Bill MacBain
MacBain & MacBain, LLC
wam@MacBainandMacBain.com

*** This is HIPAAlive! From Phoenix Health Systems ***

Aloha!

Rule of thumb: providers are like puppies. They can do anything they want, as often as they want, as long as they do it on paper.

Bill MacBain

***** Clearinghouse Document

http://snip.wedi.org/public/articles/Clearinghouse_v3.pdf

***** [hipaalive] IDENTIFIERS: Provider ID

*** This is HIPAAlive! From Phoenix Health Systems ***

I'd heard it would be a 10 digit number, makes entry via a keypad easier. I don't think a provider specifically will have more than 1 identifier number, but certainly they could have own professional identifier, and also the organization with which they are associated, for example Cardiology Associates of Central Denver, will have a provider identifier.

Christine Jensen

HIPAA Project Manager
Denver Health
303-436-7942

-----Original Message-----

From: Meg Terry [[SMTP: mterry@healthlinesystems.com](mailto:MTerry@healthlinesystems.com)]

Sent: Monday, September 24, 2001 11:20 AM

To: HIPAAlive Discussion List

Subject: [hipaalive] IDENTIFIERS: Provider ID

*** This is HIPAAlive! From Phoenix Health Systems ***

It is my understanding that the National Provider Identifier will be a 8 position alpha-numeric field. In the Proposed Rules, it states that ID's will be assigned to providers as well as organizations. Can anyone envision a provider needing more than one number -- i.e. one for him/herself and one for the organization with which they are affiliated?

Input is appreciated.

Meg L. Terry
Senior Vice President, Corporate Strategies
HealthLine Systems, Inc.
San Diego, CA

*** This is HIPAAlive! From Phoenix Health Systems ***

I read the entire discussion to envision that trading partners can maintain relationship linkages between or among two or more providers, some of which can be individual persons, and some non-persons (groups, partnerships, corporations). But, each provider would have only a single NPI.

So, Dr. Smith (NPI A1234567) and Dr. Jones (NPI A9876543) both belong to Doctors 'r US, PA (NPI B1234567). Trading partners needing to know this relationship would have to create and maintain their own relationship tables.

I would expect in submitting a service from this group, Doctor r' US to be the Billing/Pay-to provider (loop 2010AA), and Dr. Smith to be the Rendering Provider (loop 2310A).

Hal Hunter
American Medical Systems/BRB Software Systems

*** This is HIPAAlive! From Phoenix Health Systems ***

Aloha!

First, the general expectation in the industry is that the actual NPI will be all numeric and at least ten characters long, including a check digit. HHS has repeatedly noted that the NPRM Comments strongly favored such an approach (see the 11/22/2000 NPI FAQ quote below). We won't know for sure until a final rule is published, of course.

Second, my best guess is that the providers will be able to have as many NPI's as they choose to ask for. The big difference between that and our current circumstances is that the providers will get to choose, instead of the payers. See the quote below from Kepa's Myth #46 for a detailed discussion of this.

Third, the transaction standards adopted under HIPAA were developed at a time that the NPI didn't exist, and work just fine without one. There may be a few places in the implementation guides where use of the NPI itself is prescribed, rather than any of the alternatives. With luck, these will be amended in the forthcoming IG Addenda.

- Zon Owen -
(808)597-8493

<< Begin FAQ Quote >>

Updated 11/22/2000

1. What is the National Provider Identifier (NPI)?

Today, health plans assign identification numbers to health care providers -- individuals, groups, or organizations that provide medical or other health services or supplies. The result is that providers who do business with multiple health plans have multiple identification numbers. The NPI is a unique identification number for health care providers that will be used by all health plans. Health care providers and all health plans and health care clearinghouses will use the NPIs in the administrative and financial transactions specified by HIPAA. The NPI was proposed as an 8-position alphanumeric identifier. However, many commenters preferred a 10-position numeric identifier with a check digit in the last position to help detect keying errors. The NPI contains no embedded intelligence; that is, it contains no information about the health care provider such as the type of health care provider or State where the health care provider is located.

<< End FAQ Quote >>

<< Begin Kepa Quote >>

This time I will try to dispel the myth that each Provider, once the NPI becomes effective, will have only one identifier.

This is a particularly interesting myth, because the Final Rule on NPI has not been issued yet, so I am using my educated speculation to debunk a myth (in my eyes) that results from the difference between my own understanding and some other people's understanding of the proposed rules upon which we all speculate. Take it with a grain of salt. Maybe even a pinch of salt. And, if you don't think the "single NPI per provider" is a common myth, you can skip this message.

In theory, according to the NPI Proposed Rule, the NPI will be issued to each health care provider. One per provider. The same number for life, so if a provider changes careers (for example, a dentist that goes back to school to become an oral surgeon) the number stays the same. And the providers will be issued only one NPI during their lifetime.

This will be a great benefit to the entire healthcare system, as it will provide a degree of continuity of the identity that we don't have today. So, it is expected to replace the multitude of identifiers in use currently.

Today each provider has several identifiers. Each payer assigns an identifier to each provider. Medicare does it. Medicaid does it. The Blues do it. The HMOs do it. Everybody does it. And not only one, but many times the same provider will get a different identifier for each contract that he or she has with each payer. This lets the payers adjudicate the claims at different rates based on contractual provisions. And not only contracts, but some times the place where the provider works conditions the identifier to be used. For example, the downtown clinic and the suburb office or the rural facility probably have different identifiers that reflect different reimbursement rates.

To make life more challenging, the provider that has three identifiers with Medicare, probably also has three identifiers with Medicaid (different from the Medicare ones, of course) as well as three identifiers with each HMO in which he or she participates, etc. A lot of times it is many more than three. It is not unusual that the provider's billing clerk keeps a "payer book" that reflects (among other things) the different identifiers for each payer. Three ring binder, so the pages can be changed easily. I have seen some with hundreds of pages.

And, because there is no coordination on the assignment of these identifiers, they are different for each payer-provider combination.

Having said all that, not every payer lets the provider know what the internal identifiers are, so the providers end up using the Tax ID (EIN)

most of the time. I have discussed some of this last month, so I will not repeat it here.

Life would be simpler for the provider if this "multiple identity" disorder could be corrected.

The myth is that with HIPAA the provider will get only one NPI.

Some payers are up in arms about this, because with only one NPI the payer will not be able to identify the different contracts or practice locations anymore.

And I say "myth" because my understanding of the NPI, from the Proposed Rule, is a little different. Let me explain.

As I understand it, each "warm body" provider will get one and only one NPI. So far we are in sync. Also each "brick and mortar" provider will get one and only one NPI. And each "entity" provider will get one and only one NPI.

But, what is an "entity" provider? As I understand it, it is a legal entity that has a distinct legal personality. Or maybe it does not have to be "legally" unique? I am not a lawyer, so I won't elaborate. But it seems to me that "Phil Good, MD" is different from "Main Street Cardiology" and different from "Suburbia Cardiology" and different from "Big HMO Cardiology Services" and different from "Cardiology Specialists", even though all of them are different expressions of the services rendered by Dr. Good.

So, each one of those entities, under the law (and the IRS?) is a different provider that is entitled to a different NPI. So, how many "entity NPIs" can Dr. Good have? As many as he needs. As long as each one is a different "entity." And Dr. Good has control of how many "entities" he creates.

In fact, I suspect that Dr. Good downtown and Dr. Good in the rural area could be the same entity for tax reporting purposes and still be different "entities" for NPI reasons. This is only a suspicion. We will have to wait for the final rule to get the final word on this one.

The fundamental difference here is that Dr. Good is now in control. He can request as many "entity NPIs" as he needs. Again, as many as HE needs. He can tell the payer which NPI to use. In fact, Dr. Good himself becomes the coordinator of his own NPIs. In the past there was no coordination and the payers would issue NPIs as they would see fit. Now, under HIPAA, the provider will control how many NPIs he/she gets. Not the payer, but the provider makes that decision.

Of course, the provider has to make an informed decision. If the choice is to get only one NPI, there could be restrictions as to how many different contracting arrangements can be established with each payer. If the choice is to get multiple entity-NPIs the administrative burden will be higher for the provider. But it is the provider's choice.

Of course, a payer may say: If you don't have a separate entity-NPI we cannot contract with you under a separate contract. Then the provider could obtain a brand new entity-NPI, or use an existing one, or choose to do without the special contract or special reimbursement level for the rural clinic. Provider's choice.

In fact, some of these "lifetime" entity-NPIs could be "retired" by ceasing a particular business, or through mergers and acquisitions, or other reasons under the provider's control. The provider's own "warm-body" NPI will not be affected by changes in the "entity" NPI.

Business reality will, I suspect, dictate that providers obtain multiple entity-NPIs. But, instead of having three different IDs with each payer, the provider will have the same three NPIs for all payers. This is "administrative simplification" in its purest form.

I am both exaggerating and speculating here, so use your pinch of salt. But you see the trend in the discussion, right?

Of course, if all this speculation turns out to be true, the provider ID problem will be much easier to manage than it is today, and it will not cause major disruption in payer systems, other than using multiple NPIs instead of multiple internal IDs for each provider.

The final word is in the Final Rule on NPI, to be released "in the near future", so stay tuned.

Kepa Zubeldia
Claredi

<< End Kepa Quote >>

***** [hipaalive] PHI Disclosure

*** This is HIPAAlive! From Phoenix Health Systems ***

I have been watching this thread on privacy notices, consents etc with much interest. With respect to privacy notices and listing of each and every possible use or disclosure, I don't think this is what HHS had in mind. I

base this in partial from the comments section found on page 82721 towards the bottom of the middle column. The following is from that section.

: While we believe that covered entities have an independent duty to understand the laws to which they are subject, we also recognize that it could be difficult to convey such legal distinctions clearly and concisely in a notice. We therefore eliminate the proposed requirement for covered entities to distinguish between those uses and disclosures that are required by and those that are permitted by law. We instead require that covered entities describe each purpose for which they are permitted or required to use or disclose protected health information under this rule and other applicable law without individual consent or authorization. Specifically, covered entities must describe the types of uses and disclosures they are permitted to make for treatment, payment, and health care operations. They must also describe each of the purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization (even if they do not plan to make a permissive use or disclosure). We believe this requirement provides individuals with sufficient information to understand how information about them can be used and disclosed and to prompt them to ask for additional information to obtain a clearer understanding, while minimizing covered entities' burden. <?xml:namespace prefix = o ns = "urn:schemas-microsoft-com:office:office" />

A notice that stated only that the covered entity would make all disclosures required by law, as suggested by some of these commenters, would fail to inform individuals of the uses and disclosures of information about them that are permitted, but not required, by law. We clarify that each and every disclosure required by law need not be listed on the notice. Rather, the covered entity can include a general statement that disclosures required by law will be made.

Ron

```
***** [hipaalive] PRIVACY: Emailing of Patient Information
*****
*** This is HIPAAlive! From Phoenix Health Systems ***
```

Mary:

Two issues: First, it's easy for anyone with Internet access to obtain a free (non-business) copy of PGP, which meets the crypto standards quite nicely indeed. I believe most of the PGP algorithm is now in the public domain in fact.

Next, and perhaps more important, I'm not sure if your waiver is valid (legal types help me here please?). I'm not sure the patient has the ability to waive HIPAA protection on a blanket basis any more than you have

the ability to waive many of your own legal rights. For instances, I may or may not be able to agree not to pursue a specific legal action against you under certain circumstances; I cannot however waive my right to overall solutions involving the courts.

If the latter case applies, and I think that it does, your waiver may not stand up.

I'd enjoy any comments on this particularly interesting matter.

C. Jon Burke
HIPAAInfoTech
(949) 492-0442
(949) 874-6082 cell
(949) 492-6082 FAX

-----Original Message-----

From: Mary Catherine Barry [<mailto:Mbarry@hillside.com>]
Sent: Friday, September 21, 2001 9:28 AM
To: HIPAAlive Discussion List
Subject: [hipaalive] RE: PRIVACY: Emailing of Patient Information

*** This is HIPAAlive! From Phoenix Health Systems ***

Based on the readings that I have done, we were going to approach things from this perspective:

we drafted an email policy (in process of obtaining approval). In the policy it states that encryption should be used. It also states that if encryption is waived per the client's request, it must be noted on the consent that is to be obtained. We are also coming from the angle that the caseworker should

be the responsible party (after thorough training) to sit & discuss this w/ the client/family. Our expectation is that the worker will discuss thoroughly the process and they should have the feeling that the person giving consent understands what they are discussing.

The only scenarios in which we think someone may request that encryption not

be used is if (and please pardon my lack of knowledge here) they are unable to de-encrypt the email. I have the belief, as does the rest of my team, that if they truly understand that encryption is for their best interest, I don't see why they would waive the right of encryption. This is also being passed by our lawyer, but so far it looks as though if it's documented the client waived the encryption the agency should be covered. We'll see.

Mary B.

>>> wam@macbainandmacbain.com 09/10/01 11:29AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

There seems to be a consensus among the security gurus on the list that the security rules, as proposed, would prohibit transmission of PHI by unsecured e-mail. At least, they have me convinced.

As noted before, there is nothing in HIPAA that allows a patient to exempt a provider from complying with a HIPAA requirement.

The privacy rule regarding confidential communications says a provider needs to "accommodate reasonable requests." [section 164.522(b)]. My reading of the postings on this subject is that security experts would consider communication of PHI by unsecured e-mail, in violation of HIPAA security standards, an unreasonable request.

Reasonable alternatives do exist. The one I'm familiar with uses a web site. The physician or patient post messages on the site. They only have access to their own correspondence, and gain access by virtue of ID and password, which is HIPAA-acceptable. The actual transmission can be secured the way that credit card transactions on the web are secured.

Any of the security folks care to chime in with a more technical and erudite description of how this is done, please??

Bill MacBain
MacBain & MacBain, LLC
wam@MacBainandMacBain.com

-----Original Message-----

From: Mic Sager [<mailto:MSager@olympicmedical.org>]
Sent: Monday, September 10, 2001 11:10 AM
To: HIPAAlive Discussion List
Subject: [hipaalive] RE: PRIVACY: Emailing of Patient Information

*** This is HIPAAlive! From Phoenix Health Systems ***

Can someone explain why the patient's right to confidential communication does not apply here. If phone calls and snail mail are acceptable, why not e-mail. I think one could argue that regular e-mail is more secure than either of the other two. And if the patient has told us that they would like to be contacted by e-mail, how can that be disallowed?

Mic Sager

Financial Analyst/Compliance Specialist
Olympic Medical Center
360.417.7781
Fax 360.417.7739
msager@olympicmedical.org <<mailto:msager@olympicmedical.org>>

-----Original Message-----

From: Harry E. Smith [mailto:harry_e_smith@timberlinetechnologies.com]
Sent: Sunday, September 09, 2001 3:19 PM
To: HIPAAlive Discussion List
Subject: [hipaalive] RE: PRIVACY: Emailing of Patient Information

*** This is HIPAAlive! From Phoenix Health Systems ***

Hello Marvin,

You make some interesting points, but I'm not sure that I agree with your conclusions.

In the case of litigation, I assume that you are referring to the possibility of a patient suing a health care provider because an emailed message containing PHI was intercepted. The case that the plaintiff would try to make would not be that the provider broke one of the HIPAA rules, since HIPAA provides no private right of action. The plaintiff would allege that he or she suffered harm because of the interception, that the interception occurred because of something the provider did or failed to do and that the provider should reasonably have known that the interception was a possibility. The jury would be asked to award damages based on the provider's negligence.

If the provider offered the signed authorization as a defense, could the plaintiff not claim that he or she was unaware of the danger of email interception at the time the authorization was signed? Even if the document authorizing the unencrypted email contained language to the effect that emails could be intercepted by unauthorized parties, could the plaintiff not claim that he or she did not understand what this meant? To me, this seems similar to a malpractice case in which a provider performed a prohibited medical procedure - the patient's authorization would not absolve the provider of the responsibility for harm resulting from the procedure, because the provider was supposed to know better.

If I were a provider trying to convince a jury that I was not responsible for a patient's email being intercepted, I would not have absolute confidence that the signed authorization would get me off the hook;

especially since the plaintiff's attorney could show the jury that the practice of sending unencrypted emails was prohibited by a federal standard developed to prevent exactly this kind of situation.

I'm not sure what you mean when you say that the practice of sending unencrypted email is a "technical violation" of the rule. If by "technical violation" you mean a practice that is contrary to the letter of the rule but otherwise consistent with the intention of the rule, I can't see this as such an example. In the proposed security rule preamble, on Federal Register page 43255, the intention of the authors could not be more clear:

"Each organization that uses communications or networks would be required to protect communications containing health information that are transmitted electronically over open networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access systems through external communication points. When using open networks, some form of encryption should be employed."

There should be no doubt that emails traverse open networks and interceptions of such traffic are a daily occurrence. It seems to me that an HHS-OCR HIPAA compliance investigator would naturally ask a provider whether or not email was used to communicate with patients. If the provider answered in the affirmative, the next question would certainly have to do with the form of encryption in use. The purpose served would be to discover and report a HIPAA security violation.

Bye for now -- Harry

Harry E. Smith, CISSP
Timberline Technologies LLC
Telephone: 303-717-0793
Email: Harry_E_Smith@TimberlineTechnologies.com

-----Original Message-----

From: Marvin Ottinger [mailto:marvin_ottinger@hotmail.com]
Sent: Friday, September 07, 2001 10:33 AM
To: HIPAAlive Discussion List
Subject: [hipaalive] RE: PRIVACY: Emailing of Patient Information

*** This is HIPAAlive! From Phoenix Health Systems ***

Note,

Despite the purpose of the Security Rule, the consequence of breaches of any

of the HIPAA rules is some sort of penalty. From a litigation point a view, the patient's signed authorization will be an absolute defense.

And, from the HIPAA enforcement police perspective, there will be no penalty handed down for that type of technical violation of the rule. What purpose would that serve?

-MO

From: "Harry E. Smith" <harry_e_smith@timberlinetechnologies.com>
Hello Evan,

There is no provision in the HIPAA regulations whereby a patient may waive a security rule requirement. Email must be encrypted because it traverses third-party systems over which access can not be controlled by the sender nor by the receiver. The applicable section of the security regulation is §142.308(d)(1)(ii). Even if a particular patient signed a blanket authorization allowing disclosure of all of his PHI to everyone on the planet, this requirement would still apply. The security rule imposes a standard on the storage, access and transmission of data. The purpose of the security rule is to ensure the confidentiality, integrity and availability of data and services, not to protect individual patient rights.

***** H I P A A L E R T - l i t e Sept 25, 2001

=====

H I P A A L E R T - l i t e September 25, 2001

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
>Healthcare IT Consulting & Outsourcing<

=====

Subscribe free at: <http://www.hipaadvisory.com/alert/>

=====

H I P A A n e w s

*** U.S. Citizens Back Encryption Controls ***

A poll in the United States has found widespread support for a ban

on "uncrackable" encryption products, following proposals such as Sen. Judd Gregg's (R-NH) to tighten restrictions on software that scrambles electronic data. The survey, conducted by Princeton Survey Research Associates on Sept. 13 and 14, found that 72 percent of Americans believe that anti-encryption laws would be "somewhat" or "very" helpful in preventing a repeat of September 11th's terrorist attacks. Gregg is now calling for "backdoors" in encryption products, proposing that U.S. government officials have access to decryption tools when the case is deemed to be a matter of national security.

<http://hipaadvisory.com/news/index.htm#0918cnet>

*** Public Interest Groups Unite to Stop Anti-Terror
Effects on Privacy ***

The Washington Post reports a coalition of public interest groups from across the political spectrum has formed to try to stop Congress and the Bush administration from rushing to enact counterterrorism measures before considering their effect on Americans' privacy and civil rights. Tentatively named In Defense of Freedom, the group is concerned about everything from expanded electronic surveillance measures sought by the Justice Department to possible ethnic profiling in the wake of last week's terrorist attacks.

<http://www.hipaadvisory.com/news/index.htm#0918wp>

*** Reg Delays Cause Insurers to Reduce 2001 HIPAA Spending ***

According to a report this month by Managed Care Week, many insurers have decreased their 2001 HIPAA compliance budgets, saying they'll increase spending next year and in future years as the last final regs are promulgated. In second quarter SEC financial filings, publicly traded health insurers PacifiCare Health Systems, Inc. and RightChoice Managed Care, Inc., reported cuts by one third in their initial 2001 spending estimates for HIPAA compliance as a result of regulatory delays.

<http://www.hipaadvisory.com/news/index.htm#0917mcw>

H I P A A l a t e s t

NEW IN HIPAAZINE:

** So Many Choices: HIPAA Fuels Practice Management Apps Market **

PPMs were all the rage in the 1990s. But the PPM business model proved flawed, and the industry is gone save for a few single-specialty management companies. Stepping in to fill the void have been hundreds

of practice management software vendors.

<http://www.hipaadvisory.com/news/0901mp.htm>

** The Elusive CPO **

Last December, as part of HIPAA regulations, a provision was issued requiring that every patient care organization designate a chief privacy officer (CPO) to safeguard patients' personal health information--both paper and electronic. Most organizations are pondering the implications of the regulations but have done little to actually prepare for compliance by April 2003.

<http://www.hipaadvisory.com/news/Hipaazine.htm#hicpo>

NEW IN HIPAACTION:

** AHIMA Brief: Rediscovery of Patient Health Information **

<http://www.hipaadvisory.com/action/privacy/index.htm#0918ahima>

NEW IN HIPAATECH:

** Securing Your Network from Hackers: Get to Know the Enemy **

You need to be proactive in discovering the potential vulnerabilities of your network and learning about the techniques hackers employ to attack your data.

<http://www.hipaadvisory.com/tech/index.htm#0921tr>

ON THE CALENDAR:

SEPTEMBER -

THIS Wednesday, September 26th, at 2:00 p.m. EDT!

Securely HIPAA Fall Audioconference Series

Session 1: Understanding & Managing Security Assessments

For more information & to sign up NOW:

<http://www.hipaadvisory.com/ezcart/index.cfm>

OCTOBER -

Securely HIPAA Fall Audioconference Series

Session 2: Security Implementation for the Non-Technical Manager

Wednesday, October 17, 2001, at 2:00 p.m. EDT

For more information & to sign up:

<http://www.hipaadvisory.com/ezcart/index.cfm>

=====

FORWARD this posting to interested associates, who may subscribe free to HIPAAAlert at:

<http://www.hipaadvisory.com/alert/>

Subscribe to our free discussion list at:

<http://www.hipaadvisory.com/live/>

Get a weekly byte of HIPAA at:

<http://www.hipaadvisory.com/notes/>

Switch to HTML version or to text version at:

<http://www.hipaadvisory.com/signup/change.cfm>